UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of:

The premises located at 6450 N. 106th St, Milwaukee, Wisconsin and a vehicle described as a 2004 Silver Saturn Vue, VIN: 5GZCZ53434S829586. See Attachments A1 and A2.

Case No. 19-866M(NJ)

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

The premises located at 6450 N. 106th St, Milwaukee, Wisconsin and a vehicle described as a 2004 Silver Saturn Vue, VIN: 5GZCZ53434S829586. See Attachments A1 and A2.

located in the Eastern District of Wisconsin, there is now concealed:

See Attachment B.

The basis for the search under Fed. R. Crim P. 41(c) is:

- ■ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ■ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to violations of: 18 U.S.C. §§ 1030 and 875 - Computer Fraud and Interstate Communications

The application is based on these facts: See attached affidavit.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days:_____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Special Agent Lee Chartier, FBI

Printed Name and Title

Sworn to before me and signed in my presence:

Date: May 22, 2019

Judge's signature

City and State: Milwaukee, Wisconsin

Hon. Nancy Joseph, U.S. Magistrate Judge

Printed Name and Title

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Special Agent **LEE CHARTIER**, being first duly sworn, hereby depose and state as follows:

I. INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Federal Bureau of Investigation. I have been employed with the FBI since November 2007. I am currently assigned to the FBI Milwaukee Division's Computer Intrusion Task Force. Prior to becoming a Federal Agent, I worked in a variety of public and private positions in the Information Technology industry. As a Special Agent with the FBI, I investigate criminal and national security-related computer intrusion matters involving botnets, distributed denial of service attacks, the distribution of spam, malicious software, the theft of personally identifiable information, and other computer related fraud. Since joining the FBI, I have been involved in numerous criminal and national security investigations involving computer intrusions. I have received education and training in computer technology, and computer-based fraud, and I have held industry certification from Microsoft and CompTIA.

2. I am an investigative or law enforcement officer of the United States within the meaning of Title 18, United States Code, Section 2510(7); that is, an officer of the United States who is empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in Title 18, United States Code, Section 2516.

3. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for warrants to search the following:

a. the premises known as **6450 N 106th Street, Milwaukee, WI**, including the curtilage (hereinafter, **"Subject Premises"**), more fully described in Attachment A1; and

b. the vehicle described as a 2004 Saturn Vue, Silver, VIN: 5GZCZ53434S829586 (hereinafter, **"Subject Vehicle"**) more fully described in Attachment A2;

for the seizure of the items more particularly described in Attachment B, attached hereto and incorporated herein by reference, including the search of any computers, cellular telephones and/or any other electronic devices located within, for the items specified in Attachment B, and the seizure of all items in Attachment B as evidence, contraband, fruits, and instrumentalities of Title 18, United States Code, Sections 1030 (unauthorized computer access and computer-related fraud) and 875 (interstate communications) (the "Subject Offenses").

c. Title 18, United States Code, Section 1030 (unauthorized computer access and computer-related fraud) generally prohibits a person from "(a)(2) intentionally accessing a computer without authorization or exceeds authorized access and thereby obtains (C) information from any protected computer".

d. Title 18, United States Code, Section 875 (interstate communications) generally prohibits a person from "(d), with intent to extort from any person, firm, association, or corporation, any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to injure the property or reputation of the addressee or of another".

4. For the reasons set forth below, there is probable cause to believe that EJIJAH GIBSON (SUBJECT) committed the Subject Offenses. There is also probable cause to believe that the SUBJECT PREMISES is the primary residence of ELIJAH GIBSON and the SUBJECT

VEHICLE is the primary vehicle of ELIJAH GIBSON. Therefore, I respectfully submit the facts and circumstances hereafter outlined below establish probable cause to believe that at the SUBJECT PREMISES and in the SUBJECT VEHICLE, there are fruits, evidence, and instrumentalities of the Subject Offenses, to include electronic devices containing evidence of violations of Title 18, United States Code, Sections 1030 (unauthorized computer access and computer-related fraud) and Title 18, United States Code, Sections 875 (interstate communications).

5. I am familiar with the facts contained in this affidavit based upon my personal involvement in this investigation, information provided by other law enforcement agents, and private companies. Because this affidavit is submitted for the limited purpose of obtaining search warrants, I have not included each and every fact known to me concerning this investigation. I have set forth facts that I believe are necessary to establish probable cause to search the above referenced facilities.

II. PROBABLE CAUSE

A. The Investigation

6. In March 2018, SUNY Geneseo student, VICTIM-1 (an individual known to the FBI), reported to the SUNY Geneseo Police that her SnapChat account had been hacked and taken over. The subject texted VICTIM-1 from telephone number 317-386-7XXX to inform her he had taken over her account, had obtained nude photos of her, and was going to send those photos to others if she did not provide the code to get into her personal folder inside the application. VICTIM-1 provided the subject the code and he subsequently accessed more nude photos of her from this folder. At one point, the subject asked VICTIM-1, "How does it feel to get blackmailed by a fucking perve."

7. Concurrently, VICTIM-1 received notification from SnapChat indicating a new login from a "HTC Desire 530" device on 1 March 2018 at 13:15 EST. According to the SnapChat notification, the login occurred from IP address 96.72.242.133.

8. VICTIM-1 recalled that earlier on the same day, she received a "weird" SnapChat message appearing to come from her friend, VICTIM-2 (an individual known to the FBI). In the message, the individual utilizing VICTIM-2's account requested VICTIM-1 send VICTIM-2 her login and password under the pretext that VICTIM-2 wanted to post something "cute" to VICTIM-1's account. VICTIM-1 contacted VICTIM-2 separately and VICTIM-2 confirmed it was not VICTIM-2 who had sent the message and that VICTIM-2 had received (and responded) to a similar message (requesting login and password) from a friend of hers at Indiana University. VICTIM-2 advised VICTIM-1 that she had been "hacked."

9. VICTIM-2 advised she did not have nude photos saved to her SnapChat, therefore, following the "hacking" of her account, VICTIM-2 did not receive any additional messages. VICTIM-2 received notification from SnapChat that someone had logged in to her account from a new device, "HTC Desire 530" on 1 March 2018 from IP address 96.72.242.133. SnapChat also advised VICTIM-2 that a new email address had been associated to her account, foryellow456@gmail.com.

10. VICTIM-1 also received notification that her password and the associated email address had been reset on her account, effectively locking her out. According to SnapChat, the email associated to the SnapChat account was reset to forlatina456@gmail.com.

11. On June 21, 2018, FBI Buffalo conducted research via the FBI's Internet Crimes Complaint Center (IC3) in order to locate any additional complaints referencing the IP address

96.72.242.133. Research indicated a complaint was filed on February 22, 2018 by VICTIM-3 of Indianapolis, Indiana.

12. VICTIM-3's complaint indicated someone had hacked into her SnapChat account, gained access to videos and photos, and was threatening to share them. VICTIM-3 provided the subject telephone number as 317-342-2XXX and IP address as 96.72.242.133.

13. On May 24, 2018, pursuant to Grand Jury subpoena, Granite Telecommunications LLC provided information to investigating agents regarding IP address 96.72.242.133. According to Granite Telecommunications LLC, IP address 96.72.242.133 was assigned to InTown Suites Management, 887 E Main Street, Greenwood, IN, 46143.

14. On July 12, 2018, pursuant to Grand Jury subpoena, InTown Suites Management confirmed that IP address 96.72.242.133 was assigned to the Greenwood, IN property during the relevant time frame of 2/21/2018 – 3/2/2018. In addition to confirmation of the IP address, InTown Suites Management also provided investigating agents records of all registered guests at the same property (887 E Main Street, Greenwood, IN, 46143) for the same time frame.

15. On August 13, 2018, pursuant to Grand Jury subpoena, TextNow Inc[1]. provided information to investigating agents regarding telephone number 317-386-7XXX, to include:

Username: elinelson23456
Name on file: NULL
Email: elinelson23456@gmail.com
Date of birth on file: 2017-01-01
Assigned/Unassigned dates: 2018-02-22 00:59:26 / 2018-03-20 22:29:38

[1] Based on training, experience, and information provided to me by other law enforcement personnel, witnesses, and publically available sources, I know TextNow is a messaging application. The TextNow website advertises that a person can sign up for a free phone number using the "Wi-Fi only version of TextNow available for download on your own device" and if they like it, switch to a paid plan.

16. According to TextNow Inc., the telephone number 317-386-7XXX was active over a time period that corresponds to the known criminal activity.

17. On September 6, 2018, pursuant to Grand Jury subpoena, Google Inc. provided investigating agents information regarding email account elinelson23456@gmail.com, to include:

Name: Ugly Director
e-Mail: elinelson23456@gmail.com
Recovery e-Mail: eligibson85@gmail.com
SMS: +6788478XXX

18. Google Inc. also provided the following relevant IP login history for the same account:

8 consecutive Login events from IP 96.72.242.133 occurred during past 24 hours prior to the following event.
| 2018/04/08-16:03:54-UTC | 96.72.242.133 | Login |
| 2018/03/20-23:48:50-UTC | 96.72.242.133| Login |

6 consecutive Login events from IP 96.72.242.133 occurred during past 24 hours prior to the following event.
| 2018/03/16-21:48:04-UTC | 96.72.242.133| Login |

19. On October 3, 2018, pursuant to Grand Jury subpoena, Google Inc. provided investigating agents information regarding email account eligibson85@gmail.com, to include:

Name: eligibson85
e-Mail: EliGibson85@gmail.com
Recovery e-Mail: elijah.gibson12@yahoo.com
Created on: 2012/10/17-23:57:50-UTC
Terms of Service IP: 69.171.163.127, on 2012/10/17-23:57:50-UTC
SMS: +13175884XXX [US]

20. Google Inc. also provided the following relevant IP login history for the same account:

2018/04/18-00:43:13-UTC	96.72.242.133	Login
2018/04/18-00:43:13-UTC	96.72.242.133	Login
2018/04/17-14:11:44-UTC	96.72.242.133	Login

2018/04/17-14:11:44-UTC	96.72.242.133	Login
2018/04/16-23:11:04-UTC	96.72.242.133	Login
2018/04/16-23:11:03-UTC	96.72.242.133	Login
2018/04/15-08:49:00-UTC	96.72.242.133	Login
2018/04/14-07:11:10-UTC	96.72.242.133	Login
2018/04/14-07:11:08-UTC	96.72.242.133	Login
2018/04/14-02:24:31-UTC	96.72.242.133	Login
2018/04/10-08:13:52-UTC	96.72.242.133	Login

5 consecutive Login events from IP 96.72.242.133 occurred during past 24 hours prior to the following event.

| 2018/04/08-10:50:32-UTC | 96.72.242.133 | Login |

21. In sum, information provided by Google Inc. positively associates the user of email accounts EliGibson85@gmail.com and elinelson23456@gmail.com with IP address 96.72.242.133, known to be assigned to InTown Suites Greenwood, IN during the relevant time frame, and utilized in furtherance of the aforementioned crimes.

22. On August 13, 2018, FBI BF also conducted reverse social media research on e-Mail address eligibson85@gmail.com and telephone number 678-847-8XXX (as previously stated, provided by Google Inc. in response to subpoena for information regarding elinelson23456@gmail.com). This research revealed the following account associated to 678-847-8XXX:

Facebook
User ID: 100002577077764
User Name: Elijah.gibson.733
Display Name: Elijah Gibson
Gender: Male
Locations: Current City – Indianapolis, Indiana, Hometown – Milwaukee, Wisconsin.

23. A review of the Facebook profile of ELIJAH GIBSON, User ID 10000257077764, revealed GIBSON attended Vincent High School, resides in Indianapolis, Indiana, and is single. A cursory review of publicly viewable comments revealed the comment "I love you son" posted on GIBSON's profile photo by an "Angela Gibson Skinner".

24. A review of guest records provided by InTown Suites Management revealed that an ANGELA GIBSON was a guest at the property located at 887 East Main Street, Greenwood, Indiana (associated to IP address 96.72.242.133) from August 17, 2017 through April 20, 2018.

25. Investigating agents notes the dates of ANGELA GIBSON's stay at the InTown Suites property correspond to the dates of the known criminal activity as well as the login dates for both elinelson23456@gmail.com, eligibson85@gmail.com and as detailed below, Facebook account, Display Name: Elijah Gibson. The most recent login via IP address 96.72.242.133 (to the elinelson23456@gmail.com account) occurred on April 18, 2018, two days prior to ANGELA GIBSON's departure from the Greenwood property.

26. Additionally on October 3, 2018, pursuant to Grand Jury subpoena, Facebook provided information to investigating agents regarding Facebook account User ID: 100002577077764 (Display Name: Elijah Gibson), to include:

Name: Elijah Gibson
Registered Email Addresses: elijah.gibson12@yahoo.com, eligibson85@gmail.com, elijah.gibson.7330@facebook.com
Registration Date: 2011-07-07 13:06:52 UTC

27. Facebook also provided the following relevant IP login history for the same account:

IP Address 96.72.242.133, Time 2018-04-15 08:57:47 UTC
IP Address 96.72.242.133, Time 2018-04-11 05:16:08 UTC
IP Address 96.72.242.133, Time 2018-04-10 22:54:38 UTC
IP Address 96.72.242.133, Time 2018-04-06 14:19:58 UTC
IP Address 96.72.242.133, Time 2018-03-24 17:51:21 UTC
IP Address 96.72.242.133, Time 2018-03-11 18:15:00 UTC
IP Address 96.72.242.133, Time 2018-03-11 18:11:58 UTC
IP Address 96.72.242.133, Time 2018-03-11 06:00:00 UTC

28. An open source search for information relevant to ELIJAH GIBSON revealed a possible residential address of 3039 Oberlin Ct, Indianapolis, Indiana.

29. On January 11, 2019, an FBI surveillance team observed a vehicle parked in the driveway of 3039 Oberlin Ct, Indianapolis Indiana. A search performed with the Indiana Bureau of Motor Vehicles revealed the vehicle (Indiana plate AQX579) was registered to an ELIJAH NAIQUAN GIBSON, at address 3039 Oberlin Ct, Indianapolis, Indiana, 46268. Later on the same day, the FBI surveillance team observed an individual identifiable as GIBSON exit the residence, enter the vehicle registered to the same, and drive the vehicle away from the residence.

30. Following the January 11, 2019, FBI surveillance, FBI Indianapolis made multiple attempts to re-locate ELIJAH GIBSON at 3039 Oberlin Ct, Indianapolis, Indiana, all subsequent attempts to locate GIBSON at this address were unsuccessful.

31. On or about March 14, 2019, a search warrant for location based services for telephone number 317-588-4XXX was issued in an attempt to locate GIBSON after physical surveillance efforts were unsuccessful. However, it was determined GIBSON was no longer utilizing the phone, and the collection was immediately deactivated.

32. On April 23, 2019, pursuant to Grand Jury subpoena, Google Inc. provided investigating agents updated information regarding email account eligibson85@gmail.com, this include a new telephone number attributed to the account:

Name: eligibson85 .
e-Mail: EliGibson85@gmail.com
Recovery e-Mail: elinelson23456@gmail.com
Created on: 2012/10/17-23:57:50-UTC
SMS: +13177923XXX [US]

33. On May 10, 2019, pursuant to Grand Jury subpoena, T-Mobile provided investigating agents subscriber information telephone number +13177923XXX, which included the following relevant information:

Subscriber Name: ELIJAH GIBSON
Subscriber Address: 3039 OBERLIN CT INDIANAPOLIS IN 46268-1324
Subscriber Status: A
Subscriber Name Effective Date: 04/07/2018
Activation Date: 02/06/2019
Account Name: ELIJAH GIBSON
Account No: 144671442
Account Effective Date: 04/07/2018

34. On or about May 17, 2019, a search warrant for location based services for telephone number 317-792-3XXX was issued in an attempt to physically locate GIBSON. The resultant GPS ping data placed GIBSON on N. 106th St, Milwaukee, WI.

35. An open source search indicated that an ELIJAH GIBSON was associated to the address 6450 N. 106th St, Milwaukee, WI as of January 2019.

36. On May 21, 2019, FBI surveillance observed a Silver Saturn Vue bearing Indiana plate AQX579 parked at the residence.

37. Later on May 21, 2019, FBI Milwaukee affected an arrest of ELIJAH GIBSON, pursuant to an arrest warrant issued on March 12, 2019 in the Western District of New York. In a post arrest interview, GIBSON informed interviewing Agents that he had been residing at the property located at 6450 N. 106th St. since mid-February 2019.

38. Based on information more fully detailed above, investigating agents believes that ELIJAH GIBSON is the individual responsible for the unauthorized access of accounts associated to the aforementioned victims. Based on my training and experience, individuals who use electronic devices to commit fraud are likely to keep their personal electronic devices in their primary residence and in their vehicles, therefore investigating agents believes evidence of the alleged crimes will be present in electronic devices recovered from the search locations referenced above and described in Attachments A1 and A2.

B. Probable Cause Relating to the Search of the SUBJECT PREMISES and SUBJECT VEHICLE

39. Based on my training and experience, I know that searching the **SUBJECT PREMISES** further described in **Attachment A1** may provide crucial evidence of the Subject Offenses described above, including electronic devices on which the Subject Offenses were committed (ex. mobile telephones which were used to access victim social media accounts) or on which records thereof may be retained (ex. photographs saved to local drives/storage on mobile phones, thumb drives, and or computers). Based on my training and experience, I know that individuals often retain such evidence in their residences. Therefore, there is probable cause to believe evidence of the fraud will be located in the requested search locations, and that there is probable cause to seize such evidence.

40. I also know that searching the **SUBJECT PREMISES** may also provide crucial evidence of the identity of the co-conspirators of the fraud, as well as exclude the innocent from further suspicion. Based on my training and experience, I know that individuals often retain records and other documents that establish indicia of use, ownership, occupancy and/or possession of their residences, vehicles and/or items in their care, custody and control. Therefore, there is probable cause to believe these records will be in the locations to be searched, and there is probable cause to seize these records and documents, including, but are not limited to, utility and telephone bills, mail envelopes, correspondence, and identification documents, travel documents and other items more particularly described in **Attachment B**.

41. Based on my training and experience, I know that individuals who are involved in criminal activities often keep evidence of their illegal activities in their vehicles. For instance, it has been my experience that subjects leave and transport electronic devices (to include mobile

phones, laptops, and thumb drives) within their vehicles. For the above-mentioned reasons, there is probable cause to believe evidence of the Subject Offenses, including cellular telephones and other electronic devices, are also located in the **SUBJECT VEHICLE**.

C. Probable Cause Relating to Electronically Stored Evidence (ESI)

42. Based on my training and experience as well as my investigation into this matter, I know that computers, cellular telephones and other electronic devices are frequently used in the Subject Offenses, such as the offenses described above. In these types of crimes, I know that the computer, cellular telephone and other electronic devices will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. For instance, computers (including cellular telephones and other electronic devices) may contain many of the details that were used in furtherance of the offense, such as records of email accounts that were created or received communication relevant to the offense (ex. notifications from Snapchat), local and/or removable storage on which the photographs obtained as a result of the offense were saved, and/or mobile communication applications which could contain records of both the original offense and subsequent communication regarding the same. Therefore, the computer (including cellular telephone and other electronic devices) is an instrumentality of the crime because it is used as a means of committing the criminal offense as well as likely to be a storage medium for evidence of crime.

43. Here, based on a review of the evidence related to this investigation, I am aware that the Subject Offenses were committed through the use of electronic devices. After engineering his way into the victim accounts, the Subject utilized a mobile device to gain unauthorized access to the private accounts, to view the victim's photographs and videos, and to identify further victims (by exploiting the contact/friend list of the victim account). Therefore,

these devices were not only the mechanism by which the offense was perpetuated, but also likely contain evidence of the crime to include records of email notifications received following access to the victim accounts, mobile communication applications that contain text messages and/or call records detailing subsequent contact the Subject had with the victims, and photographs that the Subject viewed and likely retained following his unauthorized access of the victim accounts.

44. Based on my training and experience, I know that individuals often keep their cellular telephones, computers and other electronic devices in their residence and in their vehicles. Therefore, there is probable cause to believe that electronic devices that are instrumentalities of the crime as well as contain evidence of the crime are located within the **SUBJECT PREMISES** and **SUBJECT VEHICLE**.

II. COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

45. As described above and in **Attachment B**, this application seeks permission to search for records that might be found in the **SUBJECT PREMISES** and **SUBJECT VEHICLE** in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive, other storage media, and/or cellular telephone. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

46. I submit that if a computer or storage medium, to include cellular telephones, are found in the search locations described in above and in **Attachments A1 and A2**, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been

downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

47. As further described in **Attachment B**, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium located in the search locations described in above and in **Attachments A1 and A2** because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and

durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches

indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. As described above, a computer (including cellular telephone and other electronic devices) is an instrumentality of the crime because it is used as a means of committing the criminal offense as well as likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received;

notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

48. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on

the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

49. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

III. CONCLUSION

50. Based upon the foregoing, I submit that this affidavit supports probable cause that **ELIJAH GIBSON** committed the Subject Offenses, and that evidence of the offenses, including the electronic storage media and other physical evidence, contraband, fruits, and instrumentalities of the Subject Offenses, further described in **Attachment B**, will likely be found in and within the **SUBJECT PREMISES** and **SUBJECT VEHICLE**, more particularly described in **Attachments A1 and A2**. I respectfully request authority to search the **SUBJECT PREMISES and SUBJECT VEHICLE**, where the items specified in **Attachment B** may be found, and to seize all items listed in **Attachment B** as evidence, contraband, fruits, and

instrumentalities, as well as any other evidence, contraband, fruits and instrumentalities of the Subject Offenses, including seizing all electronic devices and searching them for the items specified in **Attachment B**.

ATTACHMENT A
(Property to be Searched)

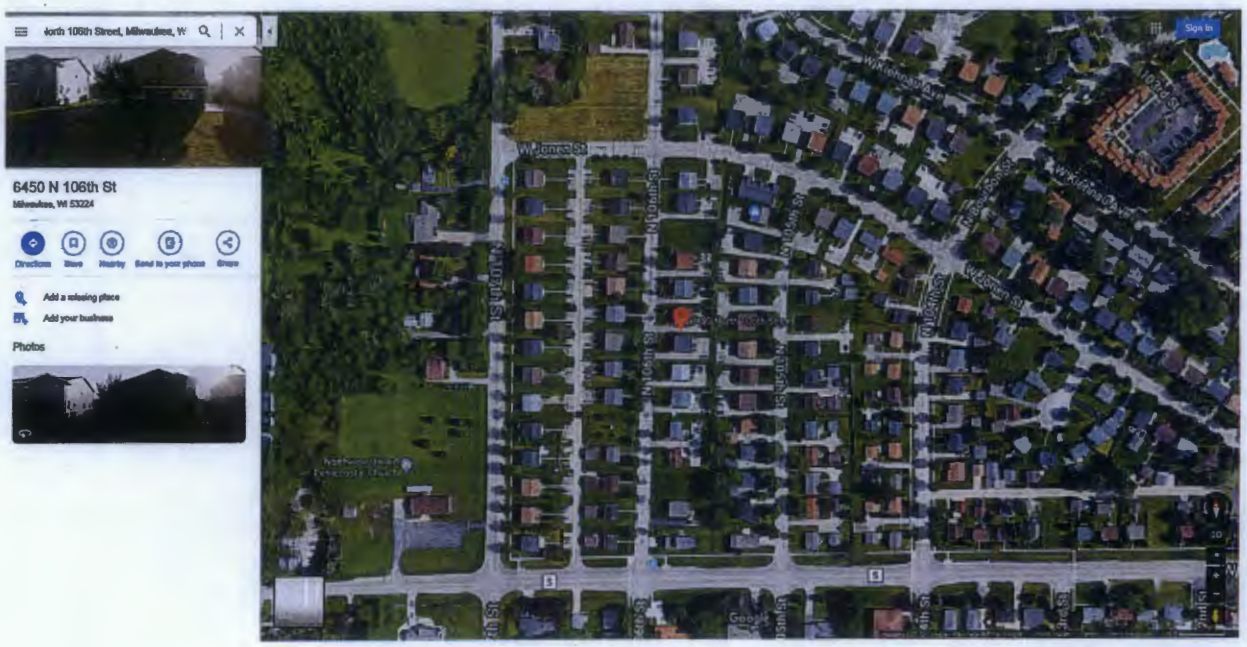
- The premises located at **6450 N. 106th St, Milwaukee, Wisconsin ("PREMISES")**, more fully described in **Attachment A1** (attached hereto and incorporated herein).

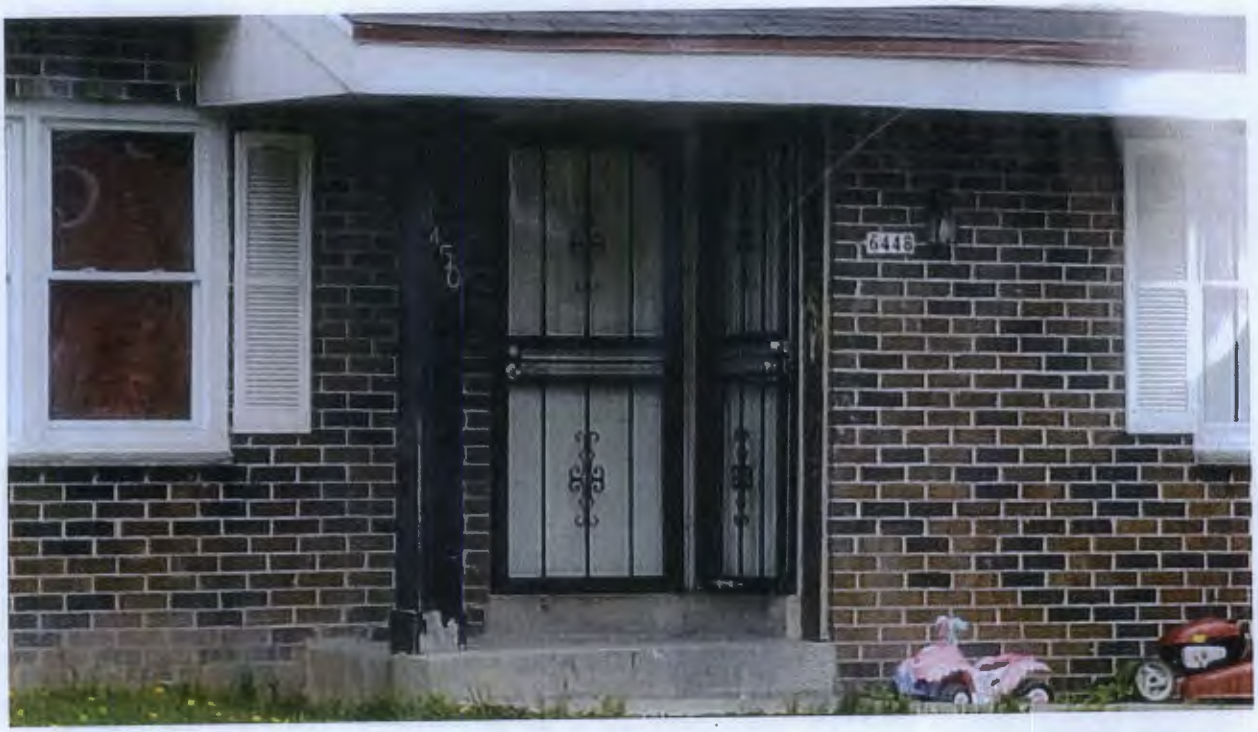
- A vehicle described as a 2004 Saturn Vue, Silver, VIN: 5GZCZ53434S829586 as more fully described in **Attachment A2** (attached hereto and incorporated herein).

Attachment A1

Premises to be Searched

The premises to be searched is 6450 N. 106th St., Milwaukee, Wisconsin, which includes the curtilage, and any garages and outbuildings on the curtilage. The residence is a two-story multi-unit bearing a combination of yellowish siding and brick façade, with white shutters and a black roof. The driveway is located to the right of the home (facing the home). The front of the house provides entry to two separate addresses (6448 N. 106th St. and 6450 N. 106th St.). The entrance to 6450 106th St. is located to the left. Attachment A1 includes photographs of the house.

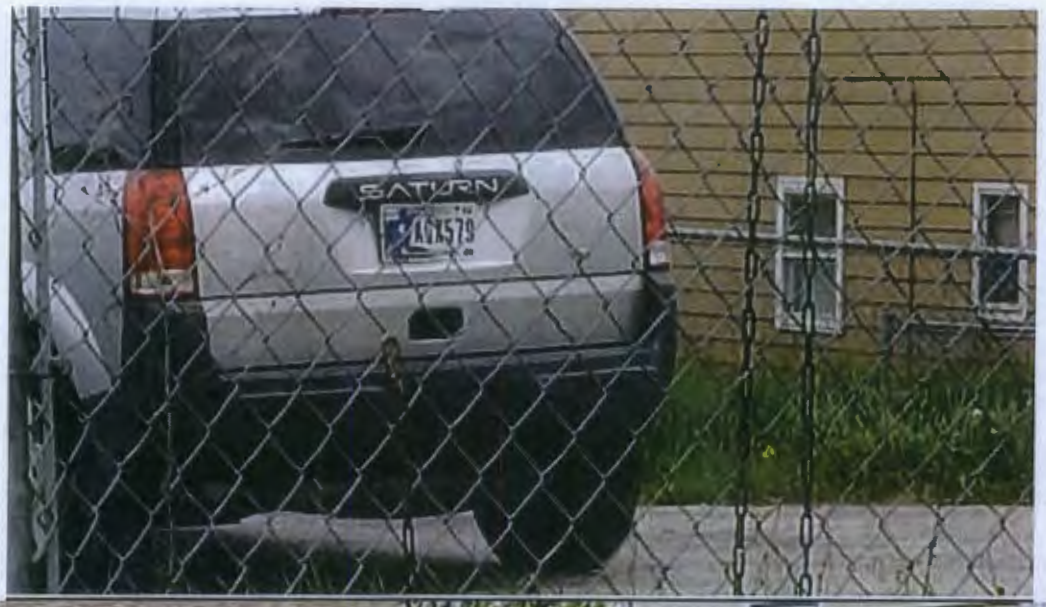


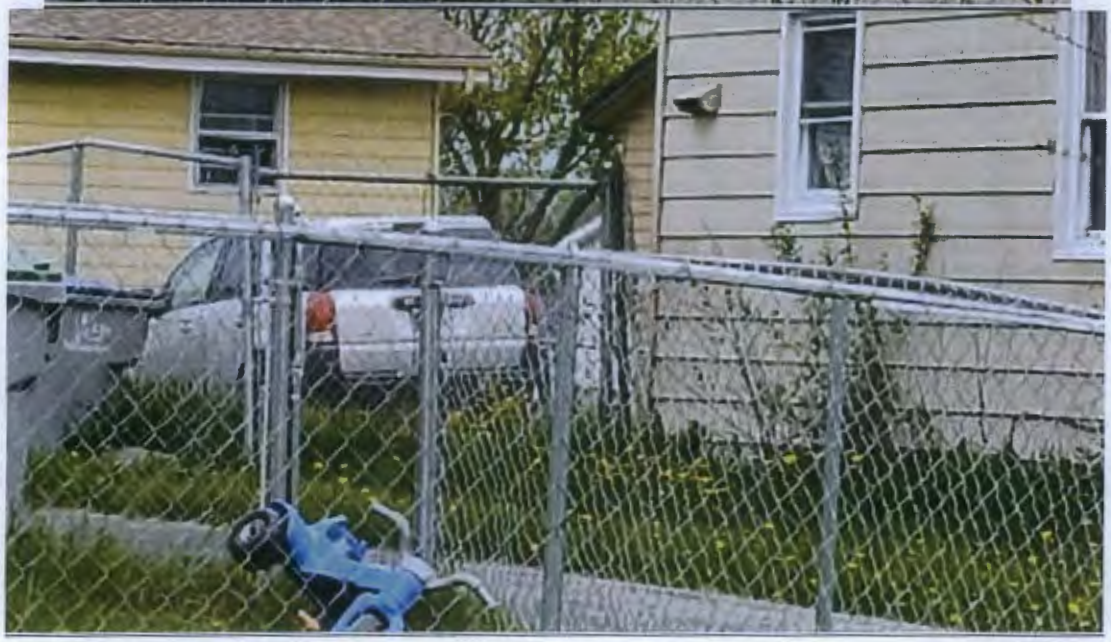

6446

ATTACHMENT A2

Description of Vehicle to be Searched

The vehicle to be searched is described as a 2004 Saturn Vue, Silver, VIN: 5GZCZ53434S829586. Attachment A2 includes photographs of the vehicle located in the driveway of 6450 N. 106th St., Milwaukee, Wisconsin.





ATTACHMENT B

Items to be Seized

A. Evidence, Fruits, and Instrumentalities of the Subject Offenses

This Warrant authorizes law enforcement agents and officers to enter the search locations specified in **Attachments A1 and A2**, including, where necessary, by means of trespass over private property, and to search for and seize from the locations specified in **Attachments A1 and A2** evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 1030 (Fraud and Related Activity in Connection with a Computer) and 875 (Interstate Communications) (the "Subject Offenses") described as follows:

1. Photographs, videos, or other personal information regarding known or potential victims;

2. All mobile telephones, smart phones, personal computers, tablet devices, other communication devices, and electronic and digital media, including compact discs, computer hard drives, SIM cards, and thumb drives, including the data stored within these devices;

3. Records, information and property concerning indicia of use, ownership, possession , or control of the search locations described in **Attachment A1 and A2**, and the items located within **Attachment A1 and A2**, including without limitation, utility and telephone bills, mail envelopes, addressed correspondence, diaries, statements, identification documents, address books, telephone directories, and keys;

4. Keys, storage combinations, passwords, and paperwork which indicate any other storage containers or facilities that could contain evidence of the Subject Offenses.

B. **Search and Seizure of Electronically Stored Information**

The items to be searched and seized from the search locations described in **Attachment A1 and A2** also include any computer devices and storage media that may contain any electronically stored information falling within the categories set forth in Section A of this Attachment above (and includes the seizure of such electronically stored information contained within), including, but not limited to, desktop and laptop computers, cellular telephones/smart phones, disk drives, routers, modems, thumb drives, personal digital assistants, digital cameras, and scanners, network equipment (the "Subject Devices"). In lieu of seizing any such computer devices or storage media, this warrant also authorizes the copying of such devices or media for later review.

The items to be seized from the search locations described in **Attachments A1 and A2** also include:

1. evidence of who used, owned, or controlled the Subject Devices at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

2. evidence indicating how and when the Subject Devices were accessed or used to determine the chronological context of device access, use, and events relating to crime under investigation and to the device user;

3. evidence indicating the Subject Device user's state of mind as it relates to the crime under investigation;

4. evidence of software that would allow others to control the Subject Devices, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

5. evidence of the lack of such malicious software;

6. evidence of the attachment to the Subject Devices of other storage devices or similar containers for electronic evidence;

7. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Subject Devices;

8. evidence of the times the Subject Devices was used;

9. passwords, encryption keys, and other access devices that may be necessary to access the Subject Devices

10. documentation and manuals that may be necessary to access the Subject Devices or to conduct a forensic examination of the Subject Devices;

11. records of or information about Internet Protocol addresses used by the Subject Devices (including port numbers);

12. records of or information about the Subject Devices' Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

13. all location history associated with the Subject Device;

14. contextual information necessary to understand the evidence described in this attachment.

Definitions

1. As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

2. The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

3. The term "storage medium" includes any physical object upon which computer data can be recorded Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

4. During the course of the search, photographs of the searched items and/or premises may also be taken to record the condition thereof and/or the location of items therein.